Ministry of planning

Central Organization for Standardization and Quality Control
Department of Conformity Evaluation for Imported Goods

Technical Division

وزارة التخطيط
الجهاز المركزي للتقييس والسيطرة النوعية
قسم تقويم المطابقة للسلع المستوردة
الشعبة الفنية

أمن المعلومات والمواصفات القياسية

أعداد المبرمج

حيدر نجم عبد جاسم

٢٠٢٤م

١٤٤٦هـ

المحتويات

إطار الدراسة :

نود أن نبين بإن هذه الدراسة " أمن المعلومات والمواصفات القياسية " قد قُدمت ضمن الخطة السنوية لقسم تقويم المطابقة للسلع المستوردة لسنة ٢٠٢٤ .

الحدود الزمانية :

تم أعداد الدراسة من ١ / ١ / ٢٠٢٤ الى ١/١٠/ ٢٠٢٤ .

الحدود المكانية :

أُعدت هذه الدراسة النظرية في دائرة السيطرة النوعية – قسم تقويم المطابقة للسلع المستوردة.

الهدف من الدراسة :

الهدف من أمن المعلومات هو حماية المعلومات من التهديدات المختلفة التي قد تؤثر عليها سواء من خلال فقدانها، أو تسريبها، أو تدميرها، أو الوصول غير المصرح به إليها. يتضمن أمن المعلومات تطبيق مجموعة من السياسات والإجراءات لضمان سرية، سلامة، وتوفر البيانات في جميع الأوقات.

أهداف أمن المعلومات تتضمن:

١- حماية سرية المعلومات :التأكد من أن البيانات غير متاحة للأشخاص غير المصرح لهم بالوصول إليها.
٢- الحفاظ على سلامة البيانات :ضمان عدم تغيير المعلومات أو تدميرها أو تعديلها بدون إذن.
٣- ضمان توفر البيانات :التأكد من أن المعلومات متاحة للمستخدمين المصرح لهم في الوقت الذي يحتاجون إليه.
٤- مكافحة التهديدات :حماية الأنظمة من الفيروسات، البرمجيات الخبيثة، والاختراقات.
٥- الامتثال للقوانين والتشريعات :التأكد من التزام المؤسسات بالقوانين الخاصة بحماية البيانات.

أما المواصفات القياسية لأمن المعلومات، فهي تشكل مجموعة من المعايير والمبادئ التي تحدد كيفية إدارة وضمان أمن المعلومات داخل المؤسسات. تعد هذه المواصفات ضرورية لتوفير إطار عمل متكامل لتحقيق أهداف الأمن.

الخلاصة :

سنتناول في هذا البحث عدة مفاهيم مرتبطة بأمن المعلومات ، مثل الفرق بين البيانات والمعلومات ، خصائص المعلومات الجيدة، مفهوم أمن المعلومات ، مراحل تطوره ، مكونات نظامه ، عناصره ، طرق ومجالات اختراقه . كما سنتناول أيضا آليات تعزيز أمن المعلومات ، حيث تعتبر سياسات أمن المعلومات أحد هذه الآليات

مُقدمة عامة :

تخيل أن يكون لديك اجتماع طارئ مع عميل محتمل وعليك أن تشرح فيه بعضا من الأمور الهامة باستخدام عرض تقديمي، وما أن بدأت كل الأنظار تتجه إليك، فوجئت بأن القرص الصلب الخاص بك وبدون مقدمات قد أتلف ولا يمكنك الوصول إلى أي معلومات؟ يبدو هذا كارثيًا، أليس كذلك، حسنًا هذا هو ما حدث فعلًا مع نائب رئيس مؤسسة مالية كبرى اثناء تجهيزه لاجتماع مهم مع إحدى العملاءالمحتملين، حيث تفاجأ بتخريب كافة معلومات القرص الخاص به مما وضعه في موقف صعب لا يحسد عليه. إذا كنت ترى هذا بمثابة كابوس صعب، أنتظر لترى ما فعله نوع من أنواع فيروس الفديه المشهور المسمى بالـ WannaCry في العديد من المنشآت والشركات لاسيما الخدمية منها، إذا تسبب هذا الفيروس في تخلى كثير من الموظفين عن الاعتماد على قواعد بياناتهم والرجوع إلى تسجيل البيانات والمعلومات في الدفاتر الورقية ومراجعتها يدويًا مع ما تشمله هذه العملية من عذاب سواء للموظفين أو للعملاء. شهدت مستشفى في ليمريك الايرلندية أيضًا واحدة من كوابيس تسرب المعلومات كذلك، عندما تفاجأ طاقم العمل في صباح يوم ما، بأن كافة المعلومات السرية والحساسة لدى المرضى قد تم نشرها علانية للعوام، ولاسيما المعلومات الخاصة بأسماء المرضى وطبيعة مرضهم والأدوية التي يحصلون عليها وتاريخهم المرضي، بالاضافة الى تاريخ ميلادهم. كل هذه السيناريوهات هي سيناريوهات حقيقية حدثت على أرض الواقع، تكبد أصحابها الكثير من الجهد والأموال في سبيل حلها وعلاج الأثار المترتبة عليها، وبعض منهم لم تستطيع التكاليف مهما بلغت أن تساعده في إنقاذ سمعته مرة أخرى أو كسب عملاء جدد بأي حال من الأحوال، وكانت جميعها نتيجة سبب واحد وهو ضعف أمن المعلومات! لذلك ومن خلال هذا الدراسة ، سنتطرق إلى عالم أمن المعلومات وما يشتمل عليه من تفاصيل، بحيث نتعرف على مفهومه وعناصره وكذلك مكوناته، بالإضافة إلى التهديدات الشائعة فيه ووسائل الحماية المعترف بها وكذلك التعرف على المواصفات القياسية الخاصة بأمن المعلومات .

الفصل الاول

الفصل الاول

١- أمن المعلومات

١ -١ مُقدمة :

يعتبر تزايد المعلومات وكثرة الاعتماد عليها من أهم السمات التي تميز العصر الحالي ، ومع التطور التكنولوجي المتسارع ، زاد الاهتمام بأمن المعلومات ، وأصبح من القضايا الهامة والرئيسية التي يهتم بها مصممي النظم ومستخدميها على السواء لضمان حماية معلوماتهم والحفاظ عليها. إن تطور تقنيات معالجة المعلومات وتداولها قد أدى إلى كثرة المعلومات وتشعبها ، مما ألقى عبئا كبيرا على المؤسسات للحفاظ على هذه المعلومات من خلال تنظيمها ، حفظها ، تحديثها ، وسرعة استرجاعها ، بالإضافة التأمينها وحمايتها . كما أن ازدياد دور نظم المعلومات والاعتماد الكبير عليها في المجالات المختلفة أدى إلى بذل الكثير من الجهود لضمان الثقة والمصداقية لهذه النظم من حيث أمنها وشفافيتها للمستخدمين .

١-٢ ما هو أمن المعلومات:

يشير مفهوم أمن المعلومات Information Security الذي يُختصر أحيانًا إلى InfoSec إلى الممارسات والأدوات التي تُستخدم في حماية البيانات الرقمية من الوصول أو التعديلات غير المصرح بها أو التعطيل أو التدمير أو السرقة، وذلك خلال نقل تلك البيانات من موقع إلى آخر أو عند تخزينها. ويوفر نظام أمن المعلومات الحماية المطلوبة للمعلومات المالية والشخصية والمعلومات الحساسة أو السرية المُخزنة في كل من الأشكال الرقمية والمادية، وبالتالي فهو يغطي مجموعة من مجالات تكنولوجيا المعلومات، ومنها البنية التحتية وأمن الشبكة والتدقيق والاختبار. وتشمل مسؤوليات ممارسات أمن المعلومات إنشاء مجموعة من العمليات التجارية التي تحمي أصول المعلومات، مع ضمان وصول أصحاب البيانات إلى بياناتهم، ومنع المتسللين من الوصول إليها [1]

١-٢-١ مجال امن المعلومات :

يعتبر مجال أمن المعلومات من أكثر المجالات الحيوية في قطاع تقنية المعلومات. والذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من كل ما يهددها. ومن زاوية تقنية، يمثل البحث عن الوسائل والادوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية. ومن زاوية قانونية، فإن أمن المعلومات محل دراسات وتدابير حماية سرية وسلامة المعلومات ومكافحة انشطة الاعتداء عليها، او استغلال نظمها في ارتكاب الجريمة، وهو هدف تشريعات حماية المعلومات من الانشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها كجرائم الإنترنت.إن موضوع أمن المعلومات يرتبط ارتباطاً وثيقا بأمن الحاسوب، وفي ظل التطورات المتسارعة في العالم التي أثرت على الامكانات التقنية المتقدمة المتاحة و الرامية إلى خرق منظومات الحاسوب بهدف السرقة أو تخريب المعلومات أو تدمير أجهزة الحاسوب، كان لا بد من التفكير الجدي بتحديد االإجراءات الدفاعية والوقائية وحسب الامكانات المتوفرة لحمايتها من أي اختراق أو تخريب، وكان على إدارة المنظمات أن تتحمل مسؤولية ضمان خلق أجواء أمنية للمعلومات تضمن الحفاظ عليها. من هنا لا بد لوزارات ومؤسسات الدولة ان تضع في اولوياته معالجة التحديين الكبيرين وهما.

---

[1]- "Information Security Management Principles," by Andy P. McHugh et al., 2013, page 1.

أولاً : التوسع في استخدام قاعة البيانات والانظمة التقنية في تقديم خدمة للمواطن، وكذلك لبناء مؤسسات الدولة وفقا لما وصل اليه العالم من التطور الكبير في هذا المجال.

ثانياً : ولغرض الحفاظ على اي مكتسب لابد لأي وزراة او مؤسسة من مؤسسات الدولة أن تضع قوانين ومتطلبات الاحتفاظ على المكتسب من الخروقات التي قد تحدث. ولابد من الاشارة الى أن الحكومة العراقية بدأت بخطوات جيدة في هذا المجال ولكن ليس بمستوى التطور الذي يشهد العالم، لذا يتطلب من الحكومة التركيز على هذا الجاب الحيوي والمهم في بناء دولة قوية وذات طابع تقني وعلمي حديث.

١-٢-٢ مهددات امن المعلومات :

هنالك عدة مصادر التي تعتبر من اكبر التهديدات لامن المعلومات ومنها مايلي:-

- الفيروسات**:** الفيروس هو برنامج صغير مكتوب بأحد للغات البرمجة ويقوم بإحداث أضرار في الحاسب والمعلومات الموجودة على الحاسب، بمعني انه يتركز علي ثلاث خواص وهي التخفي، التضاعف، وإلحاق الأذى. وتكمن مصادر الفيروس في الرسائل الإلكترونية المجهولة، وصفحات الإنترنت المشبوهة، ونسخ البرامج المقلدة، واستخدام برامج غير موثقة، كذلك تبادل وسائل التخزين دون عمل فحص مسبق مثل الأقراص والذاكرة المتنقلة وإرسال الملفات داخل الشبكة المحلية.
- تعطيل الخدمة**:** هذا النوع من التهديدات يقوم فيه القرصان أو المعتدي بإجراء أعمال خاصة تؤدي إلى تعطيل الأجهزة التي تقدم الخدمة في الشبكات (Server).
- مهاجمة المعلومات المرسلة: اعتراض المعلومات عند ارسالها من جهة إلى أخرى، وغالبا ما يحدث هذا النوع من التهديد أثناء تبادل الرسائل خلال الشبكات (Server).
- تهديدات الانترنيت: في هذا النوع يقوم القرصان بالسيطرة الكاملة على جهاز الضحية والتحكم في جميع ملفاته كما لو كانت في جهازه هو ويمكن للقرصان مراقبة الضحية بصورة كاملة. يتم الهجوم بعد أن يضع القرصان ملف صغير على جهاز الضحية (عن طريق البريد الإلكتروني أو أي وسيلة أخرى) أو عن طريق استغلال نقاط الضعف في أنظمة التشغيل.
- هجوم التضليل**:** وفيه يقوم القرصان بانتحال شخصية موقع عام. كما يمكن للقرصان أن ينتحل شخصية مستخدم موثوق به للحصول على معلومات غير مصرّحة له.
- الوصول المباشر لاسلاك التوصيل**:** في هذا النوع من التهديد يقوم المهاجم بالوصول المباشر لأسلاك التوصيل والتجسس على المعلومات المارة. ولكنه هجوم صعب ويتطلب عتاد خاص.

ولغرض التجنب اثر فقدان المعلومات والحماية الكافية لأمن المعلومات سواءً كانت في مؤسسات الدولة او المعلومات الخاصة والشخصية، فهنالك طرق عديدة لحماية هذه المعلومات ومنها ما يلي:

أ- التأمين المادي للأجهزة والمعدات.
ب- تركيب مضاد فيروسات قوي وتحديثه بشكل دوري.
ت- تركيب أنظمة كشف الاختراق وتحديثها.
ث- تركيب أنظمة مراقبة الشبكة للتنبيه الى نقاط الضعف التأمينية.
ج- عمل سياسة للنسخ الاحتياطي.
ح- استخدام أنظمة قوية لتشفير المعلومات المرسلة.
خ- دعم أجهزة عدم انقطاع التيار.
د- نشر التعليم والوعي الأمني .

١-٣ أهمية أمن المعلومات :

يدرك البشر أهمية المراقبة الدقيقة لمن يصل إلى الموارد المهمة فيقيدون ذلك بشروط وحدود واضحة، ولا ريب أن المعلومات والبيانات من أهم تلك الموارد، فيضع صاحبها قيودًا لتحديد من يستطيع الوصول إلى تلك المعلومات وكيفية وصوله إليها، من أجل ضمان أمن المعلومات التي يريد حفظها، سواء ذلك في قديم تاريخ البشرية أو حديثها، وإن كنا نركز هنا على المعنى المشهور الحديث لأمن المعلومات، وهو الأمان الرقمي للمعلومات المتداولة عبر الإنترنت وقد برزت الحاجة الملحة إلى تطوير أمن المعلومات مع التقدم التقني الواضح في كل من العتاد الحوسبي والبرمجيات التي تعمل عليها، والاعتماد المتزايد للأفراد والشركات على تقنيات المعلومات في تنفيذ عملياتها اليومية من معاملات مالية وحسابات وتوثيقات ونقل لملفات ومتابعة لسير العمليات في الشركات وغيرها، فضلًا عن المجالات الحساسة مثل المجالات العسكرية والطبية التي تتأثر أبلغ الأثر بالتلاعب فيها أو الوصول إليها لمن لا ينبغي لهم ذلك . وقد برزت الحاجة الملحة إلى تطوير أمن المعلومات مع التقدم التقني الواضح في كل من العتاد الحوسبي والبرمجيات التي تعمل عليها، والاعتماد المتزايد للأفراد والشركات على تقنيات المعلومات في تنفيذ عملياتها اليومية من معاملات مالية وحسابات وتوثيقات ونقل لملفات ومتابعة لسير العمليات في الشركات وغيرها، فضلًا عن المجالات الحساسة مثل المجالات العسكرية والطبية التي تتأثر أبلغ الأثر بالتلاعب فيها أو الوصول إليها لمن لا ينبغي لهم ذلك[٢]

١-٤ الفرق بين البيانات والمعلومات :

ان المعلومات تختلف عن البيانات ، مع أن المصطلحان يستعملان غالبا على أنهما يمثلان المعنى نفسه في حياتنا اليومية ، لذلك، فإنه من المهم توضيح الفرق بين المصطلحين قبل الدخول في مفهوم نظم وأمن المعلومات .

أ- البيانات (Data) : هي مجموعة حقائق غير منظمة قد تكون في شكل أرقام أو كلمات أو رموز لا علاقة بين بعضها البعض ، أي ليس لها معنى حقيقي ولا تؤثر في سلوك من يستقبلها . وهي المادة الخام التي تشتق منها المعلومات ، وهي تمثل (ترمز إلى) الأشياء والحقائق والأفكار والآراء والأحداث والعمليات التي تعبر عن مواقف وأفعال ، أو تصف هدفا أو ظاهرة أو واقعا معينا دون أي تعديل أو تفسير أو مقارنة ، ويتم التعبير عنها بكلمات أو أرقام أو رموز أو أشكال . مما سبق يمكن تعريف البيانات كالتالي : هي مجموعة من الحقائق الخام وغير المنظمة للمعلومات ، والتي لا يمكن الاستفادة منها إلا بعد معالجتها[٣].

ب- المعلومات (Information) : هي البيانات المجهزة في شكل منظم ومفيد وبالتالي فهي نوع من المعرفة الناتجة عن عمليات تشغيلية لخدمة أغراض بعينها . وهي البيانات المنظمة والمنسقة بطريقة توثيقية مناسبة ، بحيث تعطي معنى خاص،وتركيبة متجانسة من الأفكار والمفاهيم ، تمكن الإنسان من الاستفادة منها في الوصول إلى المعرفة واكتشافها .

المناسبة [٤].

---

[2]- Calder , Alan & Watkins , Steve (2008). IT Governance a Manager's Guide to Data Security and ISO27001/ISO 27002 (4th ed.). USA, Philadelphia : Replika Press,Pvt Ltd, p11.

[3] - Laudon, K. C., & Laudon, J. P. (2016). *Management Information Systems: Managing the Digital Firm*. Pearson, p15.

[4] -Stair, R., & Reynolds, G. (2017). *Principles of Information Systems*. Cengage Learning, p12 .

١-٥ أمن المعلومات ما قبل شبكة الإنترنت :

كانت البيانات قبل عصر الإنترنت حبيسة الغرف والبيوت والمباني، فتكون بيانات المواطنين مثلًا محفوظة في سجلات داخل مباني الدولة في المدينة أو البلدية، ولا يستطيع أحد أن يصل إليها ما لم يدخل المبنى ويطلع على السجلات، أو إلى وسائل نقل تلك البيانات من مركبات وطائرات وغيرها، أو من يستطيع التجسس على وسائل الاتصال الهاتفية أو الاجتماعات ونقل ما يجري فيها، وكان يكفي لضمان أمن المعلومات تحصين مباني السجلات وحجب تلك الاجتماعات عن الأنظار أو تقييد من يحضرها أو تمويه وسائل نقل البيانات من سيارات أو مركبات أو أفراد، أو تشفير الاتصالات الهاتفية واتصالات الراديو لحجب محتوياتها عمن يتجسس عليها.وهذا المثال لأمن المعلومات الخاصة بالدولة ينطبق على أمن المعلومات الخاص بالأفراد أيضًا، حيث لم يكن يستطيع أحد أن يطلع على محادثة بين اثنين إلا إن كان هو ثالثهما أو يتجسس عليهما، ولم يكن لأحد أن يصل إلى وثائق وصور وأموال الأفراد إلا أن استطاع دخول بيته أو اقتحامه [٥].

١-٦ أمن المعلومات بعد شبكة الإنترنت :

أما مع نقل بيئة تلك المعلومات إلى فضاء الإنترنت الواسع، فقد اتسعت دائرة التهديدات اتساعًا رهيبًا بحيث صارت وسائل الحماية التقليدية غاية في السذاجة، ووجب استحداث تقنيات تشفير للبيانات وتحقق من سلامتها، ومن يصل إليها، وتوفير سجلات ترصد تغير البيانات والتعديل فيها لمعرفة من عدَّل عليها ومتى وطبيعة التعديل الذي حدث. وباستخدام مثال سجلات الدولة في النقطة السابقة، فقد أصبحت تلك السجلات موجودة في حواسيب متصلة بالإنترنت، وعلى خوادم قد توجد داخل حدود الدولة أو خارجها -تشترط بعض الدول من شركات الحوسبة السحابية التي تستضيف سجلاتها أن تكون بيانات مواطنيها داخل حدود الدولة-

فإن استطاع شخص اختراق الوسائل الموضوعة لحماية أمن المعلومات هنا فسيصل إليها بسهولة تامة وينسخها إلى حاسوبه، حتى لو لم يكن هو نفسه داخل الدولة أو القارة حتى الموجودة فيها تلك المعلومات، على عكس ما كان يحدث من قبل إذ كان يضطر المخترق إلى التواجد في مكان تخزين تلك البيانات وتحميلها في شاحنة مثلًا.وقد يتسبب تغيير تعليمة برمجية واحدة في تهديد خطير لأمن المعلومات في الشركة أو المؤسسة يؤدي إلى تسريب بيانات العاملين في الشركة أو عملائها إلى أيدي المنافسين أو الأعداء لتلك المؤسسة، ويزيد خطر تلك الثغرات في حالة الشركات الكبرى أو التي تتعامل مع بيانات حساسة للمستخدمين كالحسابات البنكية أو البيانات الطبية [٦].

---

[5]- Parker, D. (1998). *Fighting Computer Crime: A New Framework for Protecting Information*. Wiley,p 44.

[6] -Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley,p 109.

١-٧ أدبيات امن المعلومات :

إن من أهم مفاهيم أمن المعلومات التي قد حددت بالسرية والتكامل والتوافر ومنذ أكثر من عشرين عاما، ويشار إليها بالتبادل في الأدبيات على أنها، سمات أمان، خصائص وأهداف أمنية، جوانب أساسية، معايير معلومات، خصائص معلومات هامة، واللبنات الأساسية. والمبادئ الأساسية لأمن المعلومات. والعديد من المتخصصين في مجال أمن المعلومات يؤمنون إيمانا راسخا بأن المسألة ينبغي أن تضاف كمبدأ أساسي لأمن المعلومات. وفي عام ٢٠٠٢، اقترح دون باركر(Donn Parker) نموذجا سمي ب(CIA) Confidentiality, Integrity, Availability يتكون نموذج باركر من ستة عناصر من أمن المعلومات.
العناصرهي (١) السرية، (٢) الحيازة، (٣) السلامة، (٤) الأصالة، (٥) التوفر، (٦) والأداة. وسميت هذه العناصر الستة باسم سداسي باركر اصبحت فيما بعد من اهم مواضيع للمهتمين في مجال امن المعلومات .[٧]

١-٧-١ السريةConfidentiality :

يمكن تعريف السرية في أمن المعلومات بأنها إتاحة البيانات فقط لمن لديه إمكانية الوصول المأذون بها، وفي المؤسسات، فإن الموظفين الذين يحتاجون إلى استخدام المعلومات والبيانات من أجل أداء أعمالهم هم الأشخاص المسموح لهم بالوصول إليها، وهو ما يعزز من قدرة المؤسسة على الحفاظ على سرية المعلومات الحساسة.
ولتطبيق مبدأ السرية، تقوم المؤسسة بتنفيذ تقنية تشفير البيانات وتحويلها إلى رموز ونصوص غير قابلة للقراءة حتى يتسلمها المستلم المقصود باستخدام مفتاح فك التشفير.

١-٧-٢ النزاهة Integrity :

المقصود بنزاهة البيانات سلامتها ودقتها وتوفرها بشكل كامل دون نقصان، وهو ما يفرض على المؤسسات ضرورة الحفاظ على البنية التحتية لتكنولوجيا المعلومات وتحسينها، ودعم بياناتها، والتخطيط لحماية تلك البيانات من الفقدان في حال تعرضها للاختراق.وتحتاج المؤسسات إلى تطبيق نزاهة البيانات من أجل الحفاظ على كفاءتها، وقياس أشياء مثل الإنتاجية، كما يحتاج إليها الموظفين الذين يتخذون قرارات يومية وفقًا للرؤى المستمدة من البيانات.

١-٧-٣ التوافرAvailability :

يُعد التوافر من أبرز أساسيات أمن المعلومات، والمقصود بتوافر البيانات جاهزية الشبكة والنظام والأجهزة اللازمة للاستخدام من قِبل الموظفين المأذون لهم بذلك .وتوافر البيانات يشير إلى قدرة الموظفين على الوصول إلى البيانات التي يحتاجونها في أي وقت، وهو ما قد تمنعه عدة عوامل مثل الهجمات الإلكترونية وتسريبات البيانات، وقد يؤدي ذلك إلى التوقف عن العمل.

لكن خرجت لاحقًا في التسعينات عدة إرشادات أخرى تزيد على تلك العناصر الثلاثة، وهذه العناصر مفيدة حتى للأفراد العاديين ليعلموا ما الذي يجب النظر إليه عند التعامل مع بياناتهم، ومن ثم تحديد مدى تأثير تلك

---

[7]- Parker, D. (2002). *Information Security: Principles and Practice*. Wiley,p27 .

البيانات إن وقعت في يد غير أمينة. فمثلًا، اقترح الباحث الأمني دون باركر Donn Parker في ١٩٩٨ نموذجًا بديلًا للثلاثي السابق مكونًا من ستة عناصر هي:

- سرية البياناتConfidentiality
- حيازة البيانات Possession أو التحكم فيهاControl
- سلامة البيانات وصحتهاIntegrity
- موثوقية البياناتAuthenticity
- إتاحة البياناتAvailability
- قيمة البيانات أو أثرهاUtility

والعلم بعناصر أمن المعلومات هذه مفيد حتى للأفراد العاديين، من أجل معرفة ما يجب النظر إليه في المعلومات الخاصة من صور ومستندات وجهات اتصال وغيرها، ومن ثم النظر في أوجه التعامل معها، فهل نثق في رسالة أرسلها شخص غريب إلينا أم لا -لا إلا إن كنا نعرف ذلك الشخص حقًا ورقم هاتفه أو بريده- وهل نشارك جهة اتصال مع تطبيق ثبتناه على الهاتف أم لا -لا، إلا إن كان التطبيق ذو سمعة جيدة ويحتاج حقًا إلى استخدام جهة الاتصال- وهل نأمن أن نترك الهاتف في حيازة غيرنا أم لا -لا قطعًا-، وهكذا.

١-٨ خطورة تهديدات أمن المعلومات

يكمن خطر تهديد أمن المعلومات حاليًا في سهولة الوصول إلى كميات ضخمة منها بثغرات بسيطة من ناحية، وتوفر أدوات المعالجة القوية لتلك البيانات من ناحية أخرى لاستخراج الظواهر العامة لتلك البيانات أو استقراء نتائج معينة منها، ذلك أننا أصبحنا في قرية صغيرة جدًا ويمكننا معرفة خبر حيوان انقرض في قارة أخرى تبعد عنا آلاف الكيلومترات مثلًا. وبالمثل، يمكن معرفة التوجه العام لسكان مدينة أو دولة بعينها من خلال النظر في المحادثات النصية بين أفرادها والمنشورات النصية والمرئية والمسموعة التي ينشرونها على الويب، ومن ثم استغلال تلك المعلومات في توجيههم ثقافيًا أو التأثير على الرأي العام، وخطورة مثل هذه الأساليب يكمن في سهولة الحصول على تلك البيانات وسرعة معالجتها، واستخدام أساليب مختلفة للتأثير قد لا تدركها الضحية نفسها [٨].

١-٨-١التجسس على المستخدمين :

تكون أخف الأضرار هنا هو استخدام تلك البيانات في الترويج لسلعة ما من قِبل شركة، وهو ما تفعله شركات التقنية وغيرها مع بيانات مستخدميها من خلال بيع نتائج تلك البيانات للشركات التي ترغب في بيع منتجاتها إلى مستخدمي جوجل مثلًا، لكن في تلك الحالات يكون استغلالًا غير قانوني إما بالسرقة أو بالتجسس غير القانوني على بيانات لا يريد المستخدمون استغلالها من قِبل الشركات.

١-٨-٢ التأثير على الرأي العام :

أما أسوأ الحالات ضررًا فيتمثل في التأثير على الرأي العام، مثل استخدام مزارع المستخدمين-user farmsوهي مجموعات كبيرة من المستخدمين يُوظفون لكتابة آراء ذات توجه معين عن عمد بحيث يخدم من

8- Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton & Company , p 15 .

يوظفهم وذلك من أجل كتابة آراء زائفة لمنتجات على أمازون كأبسط مثال ويمتد حتى تأييد اتجاه سياسي أو رفضه بما يُحدث زخمًا في سير الأحداث في منطقة ما، وهكذا.

١-٨-٣ استهداف المنشآت الحساسة :

باستغلال الثغرات الأمنية الرقمية أو البشرية للمعلومات في الوصول إلى نقاط حساسة في المؤسسات ومن ثم استهدافها من خلالها، كالوصول إلى حواسيب مفاعلات نووية مثلًا أو أجهزة طبية في مستشفيات أو إلى مولدات الطاقة في تلك المنشآت الطبية أو النووية، ومن ثم تعطيلها أو تخريبها أو إيقاف عملها، أو حجب الوصول إليها مقابل فدية مادية أو معنوية، ويزيد الخطر في حالة الوصول إلى منشآت عسكرية أو أنظمة دفاعية، خاصة مع ازدياد الاعتماد على الأنظمة الرقمية في الطائرات المسيرة أو أنظمة الدفاع الجوي.

١-٨-٤ سرقة الأموال :

وإن كانت الحالات المذكورة في الفقرة أعلاه نادرة الحدوث إلا أنها شديدة الخطر حال حدوثها، وتتسبب في كوارث حقيقية، لكن الحالات الأكثر شيوعًا منها تكون في استغلال ثغرات في أنظمة المعلومات البنكية التي تكون تحت سيطرة البنوك أو الشركات التي تضع يدها على وسائل دفع للمستخدمين، ومن ثم سرقة الأموال الموجودة في تلك الحسابات إما بتحويلها إلى حسابات تابعة للصوص أو استخدامها في شراء منتجات مباشرة بانتحال شخصية صاحب الحساب الأصلي.وحتى لو كانت أنظمة البنوك نفسها من التعقيد بحيث لا تسمح للمخترقين بالوصول إلى أموال المستخدمين بسهولة، إلا أن نقطة الضعف الكبرى تكمن دومًا في المستخدمين أنفسهم.

١-٨-٥ استهداف الضحايا الأفراد :

تشكل المعلومات المتوفرة حول الأفراد مصدرًا غنيًا لاستهدافهم شخصيًا إما بالسرقة أو الابتزاز أو حتى تهديد سلامتهم، من خلال الأجهزة التقنية التي يستخدمونها من حواسيب وهواتف، سواء ببيانات مباشرة مثل الصور والعناوين والبيانات المالية، أو بيانات وصفية metadata تجمعها الحواسيب والتطبيقات التي يستخدمونها، مثل المواقع الجغرافية ومواعيد الاتصالات وسجل تحركاتهم، بل وحتى تحديد وسائل تلك التحركات إن كانت باستخدام سيارات أو مشيًا على الأقدام، ومن يتعاملون معهم من أفراد أو خدمات. وتكون تلك الحالة أشد خطورة بسبب استغلال إحدى أسوأ الثغرات وأضعفها، وهي الثغرة البشرية، ذلك أن المنشآت والشركات يكون لديها أقسام وإدارات خاصة بالتعامل مع الأخطار الرقمية والأمنية، أما الأفراد ففي الغالب يغلب عليهم الجهل شبه التام بالأخطار المحيطة بهم فيما يستخدمونه من وسائل وأدوات تحمل بياناتهم ومعلوماتهم. والواقع أن العنصر البشري يمثل نقطة الضعف الكبرى في أي منظومة أمنية، لهذا تضع المؤسسات ميزانيات كبيرة للتوعية الأمنية لأفرادها تكاد تقارب الميزانيات المخصصة للأنظمة الأمنية مثل الكاميرات وبرامج مكافحة الاختراق وغيرها، وتوظف أحيانًا من يختبر كفاءة تلك المنظومات الأمنية من خلال تنفيذ اختبارات اختراق على أنظمة الشركة تحت إشرافها، أو محاكاة عمليات الاحتيال على الموظفين لاكتشاف المشاكل المحتملة ونقاط الضعف التي قد تكون لدى بعضهم من أجل معالجتها وتوعيتهم.

١-٩ وسائل حماية البيانات :

تتعدد الوسائل المتاحة لحماية أمن المعلومات والبيانات وحفظها من السرقة أو التخريب، بين الأنظمة المادية والبرمجية، والتوعية المعرفية للأفراد [٩].

١-٩-١ الحماية المادية للمعلومات :

لا شك أن أكثر مكان آمن لتخزين البيانات هو الذي لا يمكن الوصول إليه، وعلى ذلك توضع الخوادم والحواسيب التي تحتوي على بيانات حساسة في منشآت شديدة الحراسة، وتكون الحواسيب نفسها داخل غرف محصنة من الوصول غير المصرح به، وكذلك ينبغي اختيار العتاد الخاص بالحواسيب من شركات مشهورة لضمان الحصول على عتاد آمن قدر الإمكان، وتجنب شراء العتاد الرخيص إلى درجة تثير الشك، ذلك أن كثيرًا من الشركات التي تبيع عتادًا رخيصًا سواء في سوق الحواسيب أو الهواتف يتبين لاحقًا إما بتحقيقات أو بفضيحة مسربة أنها تجمع بيانات المستخدمين وتبيعها.أما على الصعيد الشخصي، فينبغي حفظ الأجهزة المنزلية التي عليها بياناتنا (الراوتر - الهاتف - الحاسوب ...إلخ.) في مأمن من العبث بها، سواء من الأطفال أو من اللصوص، واختيار كلمات مرور قوية لها، وتغييرها دوريًا كل مدة، والنسخ الاحتياطي لبياناتها لتجنب ضياعها في حالة التلف أو السرقة أو غيرها.

٢-٩-١ التوعية المعرفية للأفراد :

يجب على المؤسسة أن تنظم برامج لتوعية العاملين فيها بوسائل اختراق المؤسسة وأنظمتها للحصول على البيانات، إما باستغلال ثغرات أمنية للمؤسسة أو باستغلال الأفراد أنفسهم، حيث تتعدد وسائل اختراق المؤسسات من خلال الأفراد باستغلال جهل العنصر البشري أو بابتزازه ماديًا أو نفسيًا من خلال تهديده بفضيحة أو سرقة أو غيرها.فهنا يجب أن يُرشد الأفراد إلى كيفية الاستخدام الآمن للهواتف والحواسيب الخاصة بالعمل وكذلك الأجهزة الشخصية، لئلا يصل المخترق إلى بيانات خاصة بالموظف يستغلها في ابتزازه من أجل الحصول على معلومات خاصة بالشركة.

وهذا مفيد حتى خارج نطاق المؤسسات، فمن المهم أن يكون الوعي الرقمي منتشرًا بين أفراد المجتمع لئلا تحدث تلك الحالات على المستوى الفردي، من ابتزاز أو سرقة أو اختطاف أو غيرها، وقد نشرت شركة حسوب (اكادمية حسوب) في هذا كتابًا من خمسة عشر فصلًا في الأمان الرقمي، يشرح أهميته ومفاهيمه، وكيفية تأمين الأدوات المحيطة بالمستخدم من أجهزة أو برمجيات، والسلوكيات الصحيحة الواجب اتباعها عند تنفيذ المعاملات المالية عبر الإنترنت وعند الشعور بتهديد أو حدوث اختراق أمني.كذلك ينبغي توعية المستخدمين بأهمية البيانات الخاصة بهم، ذلك أن كثيرًا من الشركات والبرامج هذه الأيام تستخدم حيلًا نفسية للتلاعب بالمستخدمين ودفعهم إلى مشاركة بياناتهم بمحض إرادتهم، كما يحدث في كثير من التطبيقات التي تستخدم الذكاء الصناعي في محاكاة مظاهر الشيخوخة على الصور الشخصية، أو التي تطلب بيانات خاصة بالمستخدمين في صورة ألعاب بسيطة.

٣-٩-١ الحماية البرمجية في أمن المعلومات :

يُفضل اختيار البرمجيات ذات السمعة الجيدة في حماية البيانات، كالتي تستخدم تشفيرًا متقدمًا واستيثاقًا ثنائيًا للمستخدمين، والتي تنفذ نسخًا احتياطية مشفرة للبيانات بشكل دوري، إضافة إلى استخدام برمجيات الحماية من الفيروسات والبرمجيات الخبيثة وبرمجيات الفدية.

---

[٩] - القحطاني، ع .(2021) *أمن المعلومات: المفاهيم والتطبيقات* .الرياض: دار الزهراء. (ص ٤٨)

كذلك يُفضل اختيار البرمجيات المفتوحة المصدر ما أمكن إذا تساوت إمكانياتها مع البرمجيات مغلقة المصدر، ولا نشير هنا إلى أن مجانية البرامج المفتوحة، فبعضها يكون أغلى من البرامج مغلقة المصدر، لكن لإمكانية الاطلاع على شيفراتها المصدرية والتأكد أنها لا تحمل برمجيات خبيثة تضر بأمان المستخدم وبياناته.

وهذا يُطبَّق على البرمجيات بدءًا من نظام التشغيل نفسه وحتى البرمجيات والأدوات البسيطة التي تستخدمها على الهاتف أو الحاسوب، فبرنامج بسيط للمهام ToDo List لا ينبغي أن يُسمح له بتصريح الوصول إلى موقع الهاتف أو إلى الكاميرا أو بيانات المستخدم على الهاتف وجهات الاتصال مثلًا.

كما ينبغي إجراء التحديثات للعتاد الرقمي دوريًا، إذ أن الأنظمة البشرية لا تكون كاملة، وتُكتشف الثغرات كل يوم فيها فيعمل مطورو تلك الأنظمة على سدها، ثم يرسلون تحديثات أمنية إلى المستخدمين تسد تلك الثغرات لديهم كذلك.

١-١٠ ما هي مكونات نظام أمن المعلومات:

أمن المعلومات هو عبارة عن مجال تكنولوجي يتكون من ثلاثيات، فبجانب ثالوث المبادئ وثالوث العناصر الأساسية للنظام، يوجد ثالوث المكونات كذلك، وهي عناصر لا يخلو منها أي نظام أمنى خاص بالمعلومات كالآتي [١٠]:-

١-١٠-١ الأمن المادي :
يركز الأمن المادي على اللجوء إلى التدابير اللازمة للحماية المادية لكافة الأصول المستخدمة في تكنولوجيا أمن المعلومات، أي إنه العنصر المسؤول عن حماية المرافق والمعدات والموارد وكذلك الأفراد من التعرض للضرر أو الهجمات أو عمليات الوصول الغير مصرح بها، بهدف حمايتها من التخريب أو الإصابة بأي ضرر يعيق أدائها لوظيفتها الأساسية.

١-١٠-٢ الأمن الشخصي :
يقوم عنصر الامن الشخصي على التثقيف التكنولوجي المطلوب للأفراد المخول لهم الوصول إلى البيانات والأنظمة المستخدمة، إذا يقوم هذا العنصر على تعليم الأفراد أساسيات الأمن المعلوماتي بحيث لا يتعرضون لعمليات الاحتيال السبيراني أو يتسببون في تعطيل الأنظمة أو التعرض لفيروسات أو حالات اختراق نتجت عن جهل وسوء استخدام.

١-١٠-٣ أمن المنظمات :

يقوم هذا العنصر على توفير كافة الإجراءات وتدابير السلامة والحماية الخاصة بأمن وسرية المعلومات في المنظمات التي يتم استخدامها، بداية من الحفاظ على أنظمة حماية التشغيل والبرامج والتطبيقات، إلى أنظمة حماية قواعد البيانات وأنظمة حماية الدخول والولوج إلى الأنظمة وغيرها.

---

[١٠] - العمري، م .(2019) *تكنولوجيا المعلومات وأمنها* .الرياض: دار الكتاب الجامعي. (ص ٧٨) .

١-١١ الفرق بين الأمن السيبراني وأمن المعلومات:

مع ظهور الإنترنت ودخوله في كل شيء أصبح أمن المعلومات متطورًا عما سبق، وفي الوقت ذاته أكثر تهديدًا عما ذي قبل، إذا أصبحت الهجمات السيبرانية تمثل تهديدًا حقيقًا للبيانات والمعلومات وأصبح حلم وجود نظام حماية لا يحتوي على ثغرة بحلم مستحيل الحدوث. يتقاطع مفهوم أمن المعلومات مع مفهوم الأمن السيبراني في عديد من النقاط، لكن هذا لا يجعلهم يشيران إلى مفهوم واحد، إذا يمكن فهم السبب الذي يدفع البعض إلى الخلط بينهم كونها الأثنان يهدفان إلى الحفاظ على حماية المعلومات وسيرتها وتأمينها من الهجمات الضارة . إلا أن هذا التشابه لا يغنى وجود اختلافات واضحة بين هذين المفهومين وهي كالآتي:
يركز مجال أمن المعلومات على حماية المعلومات من التعرض للانتهاك أو الاختراق سواء على مستوى البيانات التي يتم تناقلها من خلال الإنترنت أو من خلال قواعد البيانات المختلفة بطريقة رقمية، أما الأمن السيبراني، فيركز فقط على أمن المعلومات التي يتم تداولها من خلال الإنترنت فحسب.
بالنسبة لتكنولوجيا أمن المعلومات فالأنظمة التي يتم استخدامها دائمًا ما يتم تطويرها ووضع خطط بديلة لها للإصلاح في حالة حدوث اختراق وتجنب تكرار الأمر مرة أخرى، أما في حالة الأمن السيبراني فيتم التركيز على حماية البيانات من الاختراق فحسب، بغض النظر عن وجود خطط بديلة في الوقت الحالي. من المميزات الأساسية لنظام أمن المعلومات هو قيامه بالتطور الذاتي والتلقائي لصد أي هجمة غير مصرح بها للأنظمة .
أما في حالة الأمن السيبراني فيتم التعامل مع الهجمات التي يعرفها النظام فحسب أما المجهولة فقد يواجه بعض الصعوبات ومن الممكن ألا يتمكن النظام من اكتشافها إلا بعد فوات الآوان وبعد حدوث الضرر الغير مرغوب فيه [١١].

١-١٢ طرق اختراق أمن المعلومات الشائعة :
لا يمنع وجود نظام أمني متكامل لحماية تكنولوجيا المعلومات من التعرض لهجمات الهاكرز من وقت لأخر، ولاسيما أن النظام العام لهذه التكنولوجيا يعد العنصر البشري فيه مكون أساسي من مكوناته، وكون الأخطاء البشرية هي الأكثر تسببًا في حدوث الاختراقات الأمنية لتكنولوجيا المعلومات دعنا نبدأ بها كأول طريقة لاختراق أمن المعلومات كالآتي [١٢].

- التعرض للتجسس من خلال تحميل البرامج والوسائط من مواقع غير آمنة تسبب في تحميل برامج خبيثة تسمح لطرف آخر بمراقبة وتسجيل أنشطة المستخدم بدون أن يعرف أو يمنح له الآذن.
- التعرض لهجمات الـ ScareWare وهي هجمات تظهر في صيغة تنكرية الهدف الظاهر منها هي مساعدتك على إصلاح النظام، إنما في الحقيقة هي من تسبب في تدميره وإتلاف البيانات الهامة فيه.
- التعرض لفيروس الفدية، وهي هجمات شهيرة تتسبب في السيطرة والتحكم الكامل على قواعد البيانات والمعلومات التي يمتلكها المستخدم وتشفيرها مقابل الحصول على مبلغ مالي مرتفع من الضحية.
- التعرض لهجمات الجذور المخفية، وهي هجمات دقيقة للغاية، حيث تستهدف الوصول إلى البيانات الخفية والحساسة للغاية في الأنظمة التي يتم مهاجمتها، بحيث تصل إلى جذور النظام بشكل كامل ومن ثم تقوم بالسيطرة عليه بحرية .

---

[1] - Stallings, W. (2019). *Network Security: Principles and Practice*. Pearson. (p. 45)

[١٢] - الأحمدي، ع .(2020) *أسس أمن المعلومات وحمايتها* .القاهرة: دار الكتب العلمية. (ص ٩٠)

- التعرض لهجمات الزومبي، وهي شكل من أشكال التجسس أيضًا لكن فيها لا تنشط الفيروسات إلا بمنح المتسللين أو الهاكرز الأمر لها بذلك، أي إن من الممكن أن يوجد على نظامك واحدة منها خامدة لا تنشط اليوم ولا بعد شهر ولا سنة، لكن فجأة وبدون مقدمات، تجد نفسك منتهك لخصوصيتك بسهولة بسبب رغبة المتسلل.
- هجمات الهندسة الاجتماعية، وهو نوع من الاحتيال الذي يعتمد على ألفة المستخدمين لمجموعة من الأسماء والشعارات والمواقع، ويقومون باستخدام هذه الألفة في دفعهم إلى زيارات روابط غير آمنة تجعلهم عرضة للاختراق بكل سهولة.
- هجمات التهديد المستمر أو ما يعرف بالـ APT وهي من أنواع الاختراق لأمن المعلومات، حيث يقوم الهاكر بمراقبة النظام والبقاء فيه لفترة طويلة بدون أن يتسبب في تعرضه للأذى أو التلف، وذلك في الحالات التي يمتلك فيها النظام المخترق ملفات مهمة وحساسة للغاية، إذا يقوم المخترق بتخزين هذه المعلومات وجمعها حتى يقوم باستغلالها فيما بعد كما يشاء، سواء بتسريبها للعامة أو بيعها للاستفادة منها.
هجمات الـ DDOS وهي نوع من الهجمات التي تستهدف التسبب بأضرار كبيرة للخوادم الخاصة بالبيانات، إذا تسبب نوع من الزيادات الغير متوقعة في حركة المرور فيها أو في إجراء سلوكيات غير طبيعية في النظام، أو رفض الخدمة الموزعة إلى شبكات أخرى أو الإبطاء أو إغلاق النظام.

- التهديدات المتعلقة باستخدام الروبوتات الخبيثة، وهي نوع من البوت التي يستهلك ثغرة أو نقطة ضعف ما في النظام المستخدم، ويقوم بإلحاق الضرر بكافة الأجهزة المتصلة بهذا النظام عن بعد، سواء بالسيطرة عليها ومراقبتها، أو بتعريضها للإتلاف أو التخريب المتعمد.
- التهديدات الداخلية من الأشخاص المخول لهم الوصول إلى المعلومات الحساسة على الأنظمة وسرقتها وتسريبها للعوام.
- ضعف أساليب الحماية المستخدمة في الأنظمة السحابية وسهولة التعرض لخداع عمليات الاحتيال التي تعتمد على المحاكاة الافتراضية لأنظمة التخزين.

١-١٣ كيفية الحماية من هجمات الهاكرز:

طبقًا لما أوردته globe newswire فإن التكلفة الإجمالية التي من الممكن أن تتكبدها الشركات بحلول عام2025 م، بسبب الهجمات الإلكترونية قد تصل إلى أكثر من 10.5 تريليون دولار سنويًا، وهو رقم لا يعد مستحيلًا إذا ربطت بين هذه التوقعات، وما بين إحصائيات الجرائم الإلكترونية المتزايدة لما يفوق الـ 600%منذ إنتشار فيروس كورونا. وللأسف، وبالرغم من زيادة التشريعات التي تفرضها الدول للحفاظ على الأمن المعلوماتى والحد من الهجمات التقنية والسيبرانية المختلفة، إلا إن عالم الهاكر في تطور هو الأخر قد يكون موازي أو يتقدم بخطوات عن عالم الحماية وأمن المعلومات. هذا التقدم لا راجع لضعف الأخير، إنما راجع لضعف الاهتمام العام بهذا المجال رغم أهميته وتأثيره الكبير سواء من الناحية الأخلاقية لما تمثله المعلومات من خصوصية، أو من الناحية المالية والسياسية التي تصبح فيه تداول بعض المعلومات بمثابة خطر قومـــــى عام.
لذلك ومن خلال تطبيق هذه النصائح، ستساهم أنت في أن تكون ضلعًا من الاضلع الفعالة في مقاومة هذه الهجمات والمساهمة في زيادة الوعي الأمنى والثقافي لما يخص أمن المعلومات:

- تحديد الجهات المخول لها الوصول إلى المعلومات واستخدام إجراءات معينة للتأكد من عدم الاحتيال وتزييف الهويات والأسماء.

- استخدام خدمات النسخ الاحتياطي والتخزين السحابي لتوافر نسخة أخرى من المعلومات في حالة التعرض لهجمات الغرض منها إتلاف وتخريب المعلومات.
- الكشف الدوري معلومات بشكل لا يسمح لأي جهة أو شخص أو النظام الوصول لها إلا الجهات المخول لها فقط.عن الثغرات والعمل على حلها قبل أن تتضخم متسببة في حدوث نتائج كارثية لا يمكن السيطرة عليها.
- زيادة الوعي بالثقافة الأمنية وتطوير المهارات التقنية الخاصة بالأفراد بحيث لا يتسبب الجهل المعلوماتي في إلحاق الضرر بالأنظمة التي يتعامل معها هؤلاء.
- استخدام أكثر من طريقة للمصادقة الآمنة عند الولوج إلى الأنظمة الخاصة.
- تفعيل جدار حماية قوي للغاية لصد أي هجمات غير متوقعة
- تطبيق برامج حماية إلكترونية لاكتشاف الفيروسات والتطبيقات الضارة.
- التطوير المستمر لتقنيات حماية أمن المعلومات بهدف مواكبتها لتهديدات الحديثة والمحتملة في المستقبل .[١٣]

١-١٤ برامج أمن المعلومات:

برامج أمن المعلومات هي البرامج المُصممة لحماية وتأمين الخوادم وأجهزة الكمبيوتر المحمولة والأجهزة المحمولة والشبكات من الفيروسات والاختراقات والوصول غير المصرح به، وتشمل تلك البرامج ما يلي :-[١٤]

أ- **برنامج الحماية من البرامج الضارة** :

يُعد برنامج الحماية من البرامج الضارة هو الحل الأمني الأفضل لمعالجة دورة الحياة الكاملة لمشكلة البرامج الضارة المتقدمة، إذ يمنع الانتهاكات ويتيح الرؤية والسيطرة للكشف سريعًا عن التهديدات واحتوائها ومعالجتها.

ب- برامج مكافحة الفيروسات :

هناك العديد من البرامج المُستخدمة في مكافحة الفيروسات المهاجمة لأجهزة الكمبيوتر أو الأجهزة المحمولة، إذ تعمل تلك البرامج على تنظيف جميع الأجهزة على الشبكة من الفيروسات لحماية البيانات الحساسة، ومن أمثلة تلك البرامجAvast free Antivirus، Norton، Kaspersky .

ج- مكافحة التجسس في أمن المعلومات :

برامج مكافحة برامج التجسس هي البرامج المُستخدمة لمكافحة التطفل على أنشطة الضحايا عبر الإنترنت ومعرفة معلوماتهم الشخصية السرية، ومنها أسماء المستخدمين وكلمات المرور، إذ تقوم تلك البرامج باكتشاف وإزالة هذه الأخطاء من النظام والحفاظ عليه آمنًا، من أجل حماية خصوصية المستخدمين والشركات والعملاء. ومن أبرز برامج مكافحة التجسس SUPERAntiSpyware ، Spybot ، SpywareBlaster و Malwarebytes.

---

[١٣] - صالح، م .(2021) .*استراتيجيات الحماية من الهجمات الإلكترونية* .الرياض: مكتبة الشروق. (ص ١١٢) .

[١٤] - الصقري، ج .(2022) .*تقنيات الكشف والوقاية من التسلل في الشبكات* .جدة: دار الفاروق. (ص ٦٨) .

د- جدران الحماية :

جدران الحماية هي برنامج يقوم بتحليل ومسحالبيانات الصادرة والداخلة لمنع الدخول غير المصرح به، وهو ما يضمن عدم تعرض بيانات المؤسسة لخطر الاختراق .ويتم تخصيص قواعد وسياسات الجدار الناري وفقًا لتفضيل المستخدم، مثل وضع استثناءات تسمح لتطبيقات معينة بالمرور عبر جدار الحماية دون وضع علامة بأنها إنذارات كاذبة.ومن أمثلة برامج جدران الحماية ManageEngine و SolarWinds Network Firewall Security Mechanism Ultimate Defenseو SolarWinds Network Firewall Management. .

هـ - برامج إدارة كلمات المرور:

وهي برامج تم تصميمها لتمكين المستخدمين من إعادة ضبط كلمات المرور الخاصة بهم في حالة قفل الحساب، إلى جانب استخدامها في مزامنة كلمات المرور، أي أنها تتيح استخدام نفس كلمة المرورعند تشغيل أكثر من تطبيق.وتفيد تلك البرامج في إنشاء كلمات مرور قوية ومميزة، وهو ما يمنع من اختراقات الحسابات التي تعتمد على ضعف كلمات المرور.ومن أبرز برامج إدارة كلمات المرور Passwordأو RoboFormأو NordPass أو.DashLane .

و- برامج الوقاية من التسلل :

تم تصميم برامج أو أدوات الوقاية من التسلل من أجل الكشف عن مناطق الضعف والتهديدات في الشبكات، إذ تستهدف تلك التهديدات تطبيقات أو خدمات معينة للسيطرة على البرامج أو الأجهزة، ولذلك فإن برامج الوقاية من التسلل تقوم بحماية النظام من خلال العمل كطبقة إضافية لتحليل البيانات التي يحتمل أن تكون خطرة، مع فحص جميع حركات المرور التي تمر عبر الشبكات. ومن أبرز تلك البرامج شبكة FireEye، ومنصة أمان شبكةMcAfee ، ونظام منع اختراق شبكة ISensor.

١-١٥ أهداف أمن المعلومات:

تتعدد الأهداف التي يسعى الأفراد والمنظمات لتحقيقها من خلال تطبيق نظام أمن المعلومات، وهي كما يلي[١٥]:

- حماية الموارد والمعلومات لضمان الأداء السلس للأنشطة التجارية والتنفيذية.
- حماية البيانات حتى في حال فقدان الأجهزة، عن طريق تشفيرها بحيث لا يمكن فك تشفيرها إلا من قِبل المستخدمين الذين لديهم مفاتيح سرية.
- توفير الحماية اللازمة لمختلف قنوات الاتصال التي تُستخدم عند الوصول إلى المعلومات.
- الحد من أضرار الهجمات الإلكترونية والسيطرة عليها حتى لا تتعطل خدمات النظام.
- الحفاظ على سرية بيانات العملاء والمنظمة، وهو ما يُكسب المنظمة سمعة جيدة في السوق التنافسي.
- استجابة المنظمات للحوادث الأمنية بطريقة أكثر فعالية وكفاءة.

[1] - Tipton, Harold F. & Krause, Micki (2006) Information Security Management Handbook (5th ed.) , United States of America : Taylor & Francis Group ،p7.

١-١٦ أهمية التشفير في أمن المعلومات:

كما سبق وذكرنا، أن التشفير هي العملية التي تحول البيانات إلى نصوص لا يمكن التعرف عليها، فهي التقنية التي تخفي البيانات باستخدام خوارزميات معقدة، ولا يمكن فك التشفير إلا بمفتاح فك التشفير الذي يحصل عليه المستخدم الذي يحمي بياناته. ويُعد التشفير في أمن المعلومات أمرًا ضروريًا لعدة أسباب وهي:

- الحماية ضد التهديدات الإلكترونية والهجمات مثل رفض الخدمة والبرامج الضارة واختراق قاعدة البيانات والوصول غير المصرح به.
- توفير الحماية للبيانات من التعرض والسرقة خلال تمريرها عبر قنوات الاتصال مثل البريد الإلكتروني.
- الحفاظ على سرية سجلات البيانات في حال تعرض الشبكة للاختراق.
- يمنع التشفير من إساءة استخدام البيانات في حال تعرض الشبكة أو مورد آخر عبر الإنترنت للهجوم من قبل البرامج الضارة أو الفيروسات.
- يُعد التشفير وسيلة تستعين بها الشركات لحماية بيانات العملاء المخزنة على محركات الأقراص الصلبة وفي أنظمة مزود الخدمة السحابية، وهو ما يعزز من ثقة العملاء في الشركات.

الفصل الثاني

الفصل الثاني

١- المواصفات القياسية الخاصة بأمن المعلومات :

٢-١ مقدمة :

يتبوأ موضوع الجودة أهمية كبيرة في مجال الإنتاج الصناعي والخدمي على حد سواء ، إذ لايمكن لأي منتوج أن ينافس المنتجات الأخرى المنافسة مالم يكن بالمستوى والجودة التي يفوق بها المنتجات المنافسة أو البديلة. فلم تعد الجودة مجرد معايير تميز المنتوج . ولا أسلوباً يتم من خلاله التعرف على مدى مطابقة المنتوج النهائي لهذه المعايير فحسب ، وإنما ذهبت إلى أبعد من ذلك لتشمل الاستخدام الأمثل للموارد المادية والبشرية واستبعاد كل معيب من أول خطوة في الإنتاج .كما إن تحقيق الجودة هو مسؤولية الجميع بدءاً من الإدارة العليا وأفراد المنظمة والمجهز وإن تحسين الجودة يؤدي إلى رفع مستوى الإنتاجية والتخلص من التكاليف الناجمة من إعادة تصنيع المنتجات المتضررة والتالفة لكي تصبح جاهزة ، وبالتالي الحصول على أقصى الأرباح والحصة السوقية الأكبر وعليه فإن الجودة تعد بمثابة السور الواقي الذي لا يمكن اختراقه ويشكل العدوان على البيئة المعلوماتية الوجه القبيح للتقنية الحديثة ، فالجرائم المتحققة عن هذا العدوان تتميز عن الجرائم العادية بسرعتها الفائقة وتأثيرها المدمر ، وقدرة مرتكبيها على الإفلات من الملاحقة والعقاب في ظل افتقاد كثير من الدول أنظمة قانونية قادرة على التعامل مع هذا العدوان والجرائم الناجمة عنه ، وتشير الإحصائيات الدولية إلى أن هناك أكثر من ملياري شخص مستخدم لأجهزة الحاسب الآلي ، فضلاً عن وجود أكثر من (13) مليار صفحة على شبكة المعلومات الدولية) الانترنت (ونحو (300) مليون موقع عليها . هكذا اتسعت البيئة المعلوماتية لتصبح ميداناً فسيحاً للعدوان عليها ولتشكل تحدياً رهيباً لمختلف الأجهزة في مواجهة هذا العدوان وما ينجم عنه من جرائم ، حيث إن ما نسبته 24%) إلى (42% من المنظمات في القطاعين الحكومي والخاص كانت ضحية لجرائم مرتبطة بالتقنية الحاسوبية ، وأن 145) إلى (730 مليون دولار سنوياً خسارة (72) شركة بسبب جرائم الحاسب الآلي ، وبينت دراسة للأمم المتحدة عن مخاطر الحاسب الآلي أن (73%) من الجرائم داخلي ، (23%)منها يرجع إلى مصادر خارجية وقدرت الخسائر الاقتصادية لهذه الجرائم عام1993) م (بنحو (2) مليار دولار ، وفي دراسة عن حالات الاختراق كوجه من أوجه العدوان على أجهزة الحكومة الامريكية لعام 1995م وجد أن هناك (250000) حالة اختراق ، 64% منها ناجحة ، وأن (1%) إلى (4%) منها تم اكتشافه. ومن أجل مواجهة هذا العدوان على البيئة المعلوماتية أصدرت المنظمة الدولية للمواصفات والمقاييس العالمية المواصفة القياسية ISO 27001 المختصة بإدارة أمن المعلومات ، ويأتي ISO 27001 كمقابل للمعيار البريطاني المعروف ببوليفيانو BS-7799

٢-٢ نشأة المواصفة القياسية:ISO 27001 :

إن المعيار الدولي السابق لأمن المعلومات كان يعرف باسم بوليفيانو BS 7799 والذي نشره معهد المقاييس البريطاني (BSI) في عام . 2000 وهو من جزئين الجزء الأول يعرف بمعيار part1 7799ويتضمن قواعد وخطوات إدارة أمن المعلومات كما تضمن المتطلبات الكلية لأمن المعلومات عن طريق أحد عشر جزءاً.

وبذلك فإن المعيار 7799-1 يعد أول معيار دولي لأمن المعلومات ، أما الجزء الثاني فيعرف بـ-2 7799أو معيار إدارة أمن المعلومات وتضمن مجموعة من المواصفات مع ارشادات لاستخدامها ، وكان يرمي إلى إدارة أمن المعلومات . أن هذا المعيار قد أستخدم داخل بريطانيا العظمى وأوروبا من قبل مئات المنظمات وحتى العام .2004 في عام 2005 المنظمة الدولية للتوحيد القياسي) أيزو (طالبت المهتمين بأمن المعلومات بتحديث أيزو2000:7799 BS ، ويحمل إسم المنظمة الدولية للتوحيد ولقد اعتمدت في ذلك على

الجزء الثاني من بوليفيانو7799 BS وبعد إجراء مجموعة من المشاورات صدرت المواصفة القياسية آيزو 17799:2005أو ما يعرف باسم أيزو27001 وهي مصممة للاستخدام من قبل أي منظمة في أي صناعة بيد أن العديد من المنظمات الصغيرة قد تواجهها بعض المشاكل تتمثل في عدم تمكنها من تلبية بعض الاحتياجات الخاصة بتدابير الدعم الدولية نظراً لمحدودية الموارد والقوى البشرية [1].
و من المهم ملاحظة أن الاسم الكامل لـ ISO 27001 هو – ISO / IEC 27001" تقنية المعلومات – تقنيات الأمان – أنظمة إدارة أمن المعلومات – المتطلبات". إن معيار الآيزو27001 ، الذي أنشأته المنظمة الدولية للمعايير (ISO) بالشراكة مع اللجنة الكهروتقنية الدولية(IEC) ، عبارة عن معيار لأمن المعلومات يوفر متطلبات نظام إدارة المعلومات .(ISMS) ويُعرّف معيار ISO 27001 ماهية نظام(ISMS) ، وما هو المطلوب إدراجه ضمن نظام إدارة أمن المعلومات، وكيف ينبغي للإدارة أن تعمل على تنفيذ ومراقبة وصيانة النظام. كما أن ISO 27001هو جزء من مجموعة المعايير المطوّرة للتعامل مع أمن المعلومات وتسمّى ب"سلسلة معايير."ISO /IEC 27000 .

٢-٣ الغرض من معيارISO 27001 :

تم تطوير معيار ISO 27001 لمساعدة جميع المؤسسات، بغض النظر عن حجمها أو مجال نشاطاتها، على حماية معلوماتها بطريقة منهجية وفعّالة، من خلال مساعدتها في تطبيق نظام إدارة أمن المعلومات (ISMS)قوي.ومن الجدير بالذكر أنّ الآيزو 27001 هو إطار شامل يُستخدم لحماية جميع أنواع المعلومات، بما في ذلك بيانات الموظفين، والبيانات المالية، وبيانات العملاء، وشروط الملكية الفكرية للشركات، والمعلومات الموكلة إلى طرف ثالث.

٢-٤ سبب أهمية شهادة الآيزو27001 :

يُوفّر المعيار المعرفة والأدوات اللازمة للمُنشآت لمساعدتها على حماية معلوماتها، كما يمكن أيضًا أن تحصل المُنشأة على شهادة ISO 27001 معترف بها دوليًا، وبذلك، تثبت لعملائها وشُركائها أنها تحمي بياناتهم وفق أفضل الممارسات.ونظرًا لأنّ معيار الآيزو 27001 معيار دوليّ، يُصبح من السهولة على المُنشأة إظهار امتثالها للمعيار في جميع أنحاء العالم، مما يزيد من فرص التعاقد مع المؤسسات الكبيرة والشركات العالمية .

٢-٥ ما هي أهداف معيار الآيزو27001 :

الهدف الأساسي من ISO 27001 هو حماية المعلومات من ثلاثة جوانب:
السرية : يحق للأشخاص المصرح لهم فقط الوصول إلى المعلومات .
النزاهة :يمكن للأشخاص المخوّلين فقط تغيير المعلومات .
التوفر :يجب أن تكون المعلومات في متناول الأشخاص المصرح لهم كلما دعت الحاجة إليها .

[1]- "ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements" [ISO.org, page 1].

٢-٦ ما هو نظام إدارة أمن المعلوماتISMS :

نظام إدارة أمن المعلومات (ISMS) عبارة عن مجموعة من القواعد التي تحتاج الشركة إلى وضعها والتأكّد من تطبيقها من أجل:

- تحديد أصحاب المصلحة وتوقعاتهم من حيث أمن المعلومات في الشركة
- تحديد المخاطر التي تُهدّد معلومات الشركة
- تحديد الضوابط وطرق التخفيف لتلبية التوقعات المحددة والتعامل مع المخاطر
- وضع أهدافًا واضحة لما يجب تحقيقه بأمن المعلومات
- تنفيذ جميع الضوابط وطرق معالجة المخاطر الأخرى
- قياس ما إذا كانت الضوابط المنفذة تعمل كما هو متوقع منها
- إجراء تحسين مستمر لجعل نظام إدارة أمن المعلومات بأكمله يعمل بشكل أفضل

يمكن تدوين هذه المجموعة من القواعد في شكل سياسات وإجراءات وأنواع أخرى من المستندات في المنظّمة، أو يمكن أن تكون في شكل عمليات وتقنيات راسخة غير موثّقة .وبشكل عام، يُحدّد معيار الآيزو 27001المستندات المطلوبة، كحد أدنى، لتطبيق نظام إدارة أمن المعلومات داخل أي منظّمة.

٢-٧ لماذا تحتاج المُنشآت لنظام إدارة أمن المعلومات :

لنظام الـ ISMS كثير من الفوائد، لكن هناك ثلاث فوائد أساسية تسعى المُنشآت إلى تحقيقها من خلال تطبيقه، وهي كالآتي:

الامتثال للمتطلبات القانونية – هناك عدد متزايد من القوانين واللوائح والمتطلبات التعاقدية المتعلقة بأمن المعلومات التي يجب على المنظّمة الالتزام بها، ويمكن حل معظمها من خلال تطبيق معيارISO 27001 ، إذ يمنحك هذا المعيار منهجية مثالية تمتثل لجميع القوانين واللوائح .اكتساب ميزة تنافسية – إذا حصلت مُنشأتك على شهادة الآيزو ولم يحصل عليها منافسيك، قد يكون لديك ميزة تنافسية تجذب بها العملاء الذين لديهم حساسية بشأن أمان معلوماتهم.انخفاض التكاليف – تتمثل الفلسفة الرئيسية لمعيار ISO 27001 في منع وقوع الحوادث الأمنية التي تُكلّف أموالًا طائلة .لذلك، ومن خلال منع وقوع تلك الحوادث، ستوفّر شركتك الكثير من المال .والخبر السار هنا أنّ تكاليف تطبيق والامتثال لـ ISO 27001 أقل بكثير من التكاليف المدفوعة في الإجراءات التصحيحية بعد وقوع الحوادث الأمنية.

٢-٨ كيف يعمل معيارISO 27001 :

ينصب تركيز معيار ISO 27001 على حماية سرية وسلامة وتوافر المعلومات في المنظّمة، ويتم ذلك من خلال معرفة المشكلات المحتملة التي يمكن أن تحدث للمعلومات) بمعنى تقييم المخاطر(، ثم تحديد ما يجب القيام به لمنع حدوث مثل هذه المشكلات) أي التخفيف من المخاطر أو معالجة المخاطر.(لذلك، تستند الفلسفة الرئيسية لـمعيار الآيزو 27001 إلى عملية إدارة المخاطر، والتي يمكن تلخيصها بـ :اكتشاف مواقع المخاطر، ثم معالجتها بشكل منهجي، من خلال تنفيذ ضوابط الأمان المذكورة بالمعيار.يتطلب معيار ISO 27001 من الشركة إدراج جميع الضوابط التي سيتم تنفيذها في مستند يسمى بيان قابلية التطبيق[٢].

[٢] - ISO 27001 نظام إدارة أمن المعلومات الصفحة ٤ .

٢-٩ ما هي متطلبات معيارISO 27001 :

تتمثّل المتطلبات الإلزامية لمعيار- ISO 27001 في البنود من 4 إلى10 ، وهذا يعني أنه يجب تنفيذ جميع هذه المتطلبات في المُنشأة التي تُريد الامتثال للمعيار .كما يجب تنفيذ الضوابط الواردة في" الملحق أ "فقط إذا تم التصريح بأنها قابلة للتطبيق في بيان قابلية التطبيق.يمكن تلخيص المتطلبات من الأقسام من 4 إلى 10 على النحو التالي:

البند :4 سياق المنظمة – يحدد متطلبات فهم القضايا الخارجية والداخلية، والأطراف المعنية ومتطلباتهم، وتحديد نطاق نظام.ISMS

البند :5 القيادة – تحدد مسؤوليات الإدارة العليا، وتعيين الأدوار والمسؤوليات، ومحتويات سياسة أمن المعلومات عالية المستوى.

البند :6 التخطيط – يحدد متطلبات تقييم المخاطر، ومعالجة المخاطر، وبيان قابلية التطبيق، وخطة معالجة المخاطر، وتحديد أهداف أمن المعلومات.

البند :7 الدعم – يحدد متطلبات توفر الموارد والكفاءات والوعي والاتصال والتحكم في المستندات والسجلات.

البند :8 التشغيل – يحدد آلية تنفيذ تقييم المخاطر ومعالجتها، وكذلك الضوابط والعمليات الأخرى اللازمة لتحقيق أهداف أمن المعلومات.

البند :9 تقييم الأداء – يحدد متطلبات المراقبة والقياس والتحليل والتقييم والتدقيق الداخلي ومراجعة الإدارة.

البند :10 التحسين – يحدد متطلبات القيام بعمليات عدم المطابقة والتصحيحات والإجراءات التصحيحية والتحسين المستمر.

٢-١٠ ضوابطISO 27001 :

ضوابط معيار الآيزو 27001 هي عبارة عن الممارسات التي يجب تنفيذها لتقليل المخاطر إلى مستويات مقبولة، ويمكن أن تكون تلك الضوابط :تقنية أو تنظيمية أو قانونية أو مادية أو بشرية، إلخ..

٢-١١ كيف تُطبّق ضوابط معيارISO 27001 :

يتم تنفيذ الضوابط الفنية بشكل أساسي في أنظمة المعلومات، باستخدام مكونات البرامج والأجهزة والبرامج الثابتة المضافة إلى النظام .على سبيل المثال النسخ الاحتياطي وبرامج مكافحة الفيروسات وما إلى ذلك.

يتم تنفيذ الضوابط التنظيمية من خلال تحديد القواعد الواجب اتباعها والسلوك المتوقع من المستخدمين والمعدات والبرامج والأنظمة .على سبيل المثال، سياسة التحكم في الوصول، سياسة استخدام الأجهزة الشخصية في العمل"BYOD" ، إلخ..

يتم تنفيذ الضوابط القانونية من خلال ضمان اتباع القواعد والسلوكيات المتوقعة وإنفاذ القوانين واللوائح والعقود وغيرها من الأدوات القانونية المماثلة التي يجب على المنظمة الامتثال لها .على سبيل المثال اتفاقية عدم الإفصاح(SLA) ، اتفاقية مستوى الخدمة(NDA) ، إلخ.

يتم تنفيذ الضوابط المادية بشكل أساسي باستخدام المعدات أو الأجهزة التي لها تفاعل مادي مع الأشخاص والأشياء .على سبيل المثال :كاميرات المراقبة، وأنظمة الإنذار، والأقفال، وما إلى ذلك.

يتم تنفيذ ضوابط الموارد البشرية من خلال توفير المعرفة والمهارات والخبرات اللازمة للأشخاص لتمكينهم من أداء أنشطتهم وأدوارهم في المُنشأة بطريقة آمنة .على سبيل المثال، إجراء تدريب توعوي أمني، أو تدريب المدقق الداخليISO 27001 ، إلخ..

٢-١٢ من يمكنه الحصول على شهادة نظام إدارة أمن معلومات ISO 27001 :

تعد شهادة ISO 27001 المتخصصة في نظام إدارة أمن المعلومات مناسبة لمختلف أشكال المؤسسات، سواء كانت صغيرة أو كبيرة، وأيا كان المكان الذي تتواجد فيه تلك المؤسسات حول العالم.وتلك الشهادة هي وثيقة لا غنى عنها بالنسبة للشركات والمؤسسات التي تعمل في قطاعات تحظى فيها المعلومات بأهمية خاصة، ومن أبرزها القطاعات الصحية، المالية والأخرى المرتبطة بتكنولوجيا المعلومات.ولا يشترط أن يكون لدى المؤسسات أو الشركات ميزات بعينها لتتمكن من إنشاء نظام إدارة أمن المعلومات آيزو ٢٧٠٠١، بل يمكن لأي مؤسسة، سواء خاصة أو عامة، أن تباشر في تثبيت النظام، ومن ثم الحصول على شهادة إدارة أمن معلومات ISO 27001 لتلبية احتياجاتها بكافة النشاطات.لإنشاء نظام إدارة أمن معلومات ISO 27001 ، لا تحتاج المؤسسات إلى ميزات محددة. يمكن لأي مؤسسة تعمل في القطاع العام أو الخاص تثبيت هذا النظام من أي حجم والحصول على شهادة. تلبي معايير ISO 27001 احتياجات المنظمة في كل بُعد وفي كل مجال من مجالات النشاط[٣] .

٢-١٣ فوائد شهادة ISO 27001 :

- **تطوير وتحسين أمن المعلومات :**يتم ذلك من خلال مساعدة شهادة الايزو ٢٧٠٠١ المؤسسات على تحديد المخاطر الأمنية وتطوير إجراءات الأمن المناسبة للوقاية منها والتعامل معها، الأمر الذي يؤدي في نهاية المطاف إلى تطوير أمن المعلومات.
- **ثقة أكبر بين المؤسسة والعملاء :**تفيد شهادة ايزو ٢٧٠٠١ في زيادة الثقة بين العملاء والشركاء والمستثمرين. إذ أنها دليل قوي يشير إلى التزام المؤسسة بحفظ سرية المعلومات وحمايتها بأفضل الوسائل المتاحة.
- **تنظيم الإدارة وتحسينها :**تساعد شهادة ISO 27001 في تنظيم إدارة المؤسسة وتحسينها من خلال إجراءات وأنظمة واضحة.
- **مطابقة المتطلبات القانونية :**تشير شهادة الآيزو ٢٧٠٠١ إلى امتثال المؤسسة للمتطلبات القانونية والتنظيمية المتعلقة بأمن المعلومات و**زيادة شعبية الشركة ورفع سمعتها :**يساعد هذا البند في تطوير عمل المؤسسة وجلب المزيد من العملاء مما يعني تحقيق أرباح إضافية.

٢-١٤ معايير أمن المعلومات - نظرة عامة

في الأوقات التي يتم فيها تداول البيانات والمعلومات مثل السلع ، من الضروري حمايتها. تتمثل إحدى طرق القيام بذلك في تنفيذ إدارة أمن المعلومات بناءً على سلسلة معايير أمن المعلومات ISO / IEC 2700x. هذه مجموعة معايير دولية لأمن تكنولوجيا المعلومات وأمن المعلومات في المنظمات الخاصة أو العامة أو غير الهادفة للربح. استنادًا إلى ISO 27001 ، يمكن تنفيذ نظام إدارة أمن المعلومات (ISMS) ، والذي يمكن للمنظمات والسلطات العامة إنشاؤه وتشغيله واعتماده لحمايتهم.

٢-١٥ أمن المعلومات: مجموعة معايير ISO 2700X :

[3]- **ISO 27001** - متطلبات أنظمة إدارة أمن المعلومات، ISO/IEC 27001:2013 ، p 13 .

تتعامل المعايير الفردية لأمن المعلومات في سلسلة ISO 2700x مع مواضيع متنوعة في مجال أمن المعلومات. على سبيل المثال ، تحدد المواصفة القياسية الدولية ISO 27001 نظام إدارة أمن المعلومات (ISMS) .

- ISO 27701 نظام إدارة حماية البيانات .
- ISO 27017 إرشادات حول تدابير أمان المعلومات للحوسبة السحابية .
- ISO 27005 إرشادات لإدارة مخاطر أمن المعلومات.

تتطلب شهادةISO 27001 ، على سبيل المثال من DQS ، قدرًا معينًا من الإعداد والجهد. ومع ذلك ، تقدم الشركة دليلاً موثقًا على امتثالها لمتطلبات أمن المعلومات وتنفيذ تدابير لحماية بيانات الشركة الحساسة. هذه ميزة تنافسية واضحة [٤].

هنالك عشرة معايير ISO بشأن أمن المعلومات يجب أن تكون على دراية بها

توفر القائمة أدناه نظرة عامة إعلامية عن الحالة الحالية لسلسلة معايير ISO 2700x في أمن المعلومات. جميع المعايير متاحة للشراء من.ISO website

- ISO 27001 متطلبات أنظمة إدارة أمن المعلومات :

في الأوقات التي يتم فيها تداول البيانات والمعلومات مثل السلع النادرة ، تكون حمايتها ضرورية. يتم توفير الأساس الأمثل للتنفيذ الفعال لاستراتيجية أمنية شاملة من خلال نظام إدارة أمن المعلومات حسن التنظيم (ISMS) وفقًا للمعيار .ISO 27001 هذا معيار معترف به دوليًا لأمن المعلومات في المنظمات الخاصة أو العامة أو غير الهادفة للربح ، والذي لا يغطي فقط جوانب أمن تكنولوجيا المعلومات.

ISO / IEC 27001: 2013تكنولوجيا المعلومات - تقنيات الأمن - أنظمة إدارة أمن المعلومات - المتطلبات

- ISO 27019 تدابير أمن المعلومات لإمدادات الطاقة :

ال ISO 27019 يصوغ معيار أمن المعلومات تدابير تكميلية لقطاع صناعة الطاقة.

ISO/IEC 27019:2017تكنولوجيا المعلومات - تقنيات الأمن - ضوابط أمن المعلومات لصناعة مرافق الطاقة

يساعدك على تأمين أنظمة التحكم في العمليات الإلكترونية المستخدمة للتحكم في إنتاج ونقل وتخزين وتوزيع الطاقة الكهربائية والغاز والزيت والحرارة والتحكم في العمليات الداعمة ذات الصلة ومراقبتها.

ما يمكنك فعله بالمعيار:

- التأكد بشكل منهجي من أهداف الحماية المتمثلة في سرية المعلومات وتوافرها وسلامتها.
- تحسين مستوى الأمان بشكل مستمر ومقاومة الوصول غير المصرح به.

[4]- ISO/IEC 27002:2022.

- تحقيق قدر أكبر من الأمان للعمل واليقين القانوني ، وتحسين الالتزام بمتطلبات الامتثال ذات الصلة.
- زيادة الوعي الأمني بين الموظفين والمديرين.
- تحقيق درجة عالية من الثقة والولاء بين جميع الأطراف المهتمة.
- أظهر دليلًا معترفًا به على فعالية تدابيرك الأمنية للسلطات ، مثل وكالة الشبكة الفيدرالية الألمانية(BNetzA) .

- ISO 27006 متطلبات جهات منح الشهادات :

تهدف ISO 27006 إلى هيئات مثل DQS التي تقدم شهادات لأنظمة إدارة أمن المعلومات. يصف معيار الاعتماد ISO 27006 المتطلبات التي يجب على هيئات إصدار الشهادات اتباعها عند تقييم أنظمة إدارة عملائها إلى ISO 27001 للحصول على الشهادة.

ISO/IEC 27006:2015تكنولوجيا المعلومات - تقنيات الأمن - متطلبات الهيئات التي تقدم التدقيق ومنح الشهادات لأنظمة إدارة أمن المعلومات

وهذا يشمل على سبيل المثال إثبات جهود المراجعة المحددة أو المواصفات الخاصة بمؤهلات المراجعين. تضمن عمليات الاعتماد الموضحة في المعيار أن شهادات ISO 27001 الصادرة عن هيئات إصدار الشهادات المعتمدة تتمتع بصلاحية دولية.

- ISO 27002 إرشادات حول ضوابط أمن المعلومات :

يحتوي نظام إدارة أمن المعلومات (ISMS) وفقًا لمعيار ISO 27001 على ملحق معياري أ: أهداف وضوابط التدبير المرجعي.

ISO/IEC 27002:2022أمن المعلومات والأمن السيبراني وحماية الخصوصية - ضوابط أمن المعلومات

يحتوي هذا الملحق على تدابير محددة ليتم تنفيذها كجزء من نظام الإدارة ، حسب الصلة بالمنظمة . ISO 27002هو دليل مع توصيات لتنفيذ التدابير من.ISO 27001

- ISO 27000 نظرة عامة ومفردات أنظمة إدارة أمن المعلومات :

يحتوي ISO 27000 على المصطلحات والتعريفات المستخدمة في سلسلة معايير .ISO 2700X يوفر ISO 27000 نظرة عامة على أنظمة إدارة أمن المعلومات وسلسلة معايير ISO 2700x مع معايير أمن المعلومات الخاصة بهم.

ISO/IEC 27000:2018تكنولوجيا المعلومات - تقنيات الأمن - نظم إدارة أمن المعلومات - نظرة عامة والمفردات

في مسرد المصطلحات ، يتم تعريف المصطلحات (الفنية) بشكل صريح ورسمي.

- ISO 27701 إرشادات بشأن إدارة حماية البيانات :

معيار أمن المعلومات المرتبط على وجه التحديد بخصوصية البيانات ISO 27701 يحدد نظام إدارة حماية البيانات بناءً على ISO 27001 و ISO 27002 (ضوابط أمان المعلومات) و ISO 29100(إطار عمل خصوصية البيانات) للتعامل بشكل مناسب مع كل من معالجة البيانات الشخصية وأمن المعلومات. ينطبق هذا على كل من وحدات التحكم والمعالجات للبيانات الشخصية.

ISO/IEC 27701:2019-08تقنيات الأمان - امتداد ISO / IEC 27001 و ISO / IEC 27002لإدارة معلومات الخصوصية - المتطلبات والإرشادات

- ISO 27017 دليل لتدابير أمن المعلومات في الخدمات السحابية :

يوفر معيار ISO 27017 إرشادات حول إجراءات أمان المعلومات في الحوسبة السحابية ضمن معايير أمن المعلومات.

ISO/IEC 27017:2015تكنولوجيا المعلومات - تقنيات الأمان - قواعد الممارسة الخاصة بضوابط أمن المعلومات على أساس ISO / IEC 27002 للخدمات السحابية

توصي وتدعم وتوفر تدابير إضافية لتنفيذ ضوابط أمان المعلومات الخاصة بالسحابة .

- ISO 27018 إرشادات بشأن حماية البيانات في الخدمات السحابية :

يوفر معيار ISO 27018 إرشادات للتأكد من أن موفري الخدمات السحابية يقدمون ضوابط أمان المعلومات المناسبة لحماية خصوصية عملائهم من خلال تأمين البيانات الشخصية الموكلة إليهم.

ISO/IEC 27018:2019تكنولوجيا المعلومات - التقنيات - قواعد الممارسة لحماية معلومات التعريف الشخصية (PII) في السحب العامة التي تعمل كمعالجاتPII

يتبع هذا المعيار ISO 27017 (تدابير أمان المعلومات في الخدمات السحابية) ، والتي تغطي جوانب أمان المعلومات الأخرى للحوسبة السحابية بدلاً من حماية البيانات فقط.

إليك ما يمكنك فعله بالمعيار:

حدد ضوابط حماية PII كجزء من تنفيذ نظام إدارة أمن معلومات الحوسبة السحابية على أساس ISO 27001.

- ISO 27005 إرشادات حول إدارة مخاطر أمن المعلومات :

يوفر معيار ISO 27005 إرشادات حول إدارة مخاطر أمن المعلومات ويدعم المفاهيم العامة حول هذا المنصوص عليها في.ISO 27001

ISO/IEC 27005:2018-07تكنولوجيا المعلومات - تقنيات أمن تكنولوجيا المعلومات - إدارة مخاطر أمن المعلومات.

يهدف ISO 27005 أيضًا إلى دعم تنفيذ أمن المعلومات بناءً على مفهوم إدارة المخاطر.

- ISO 27007 دليل لتدقيقISMS :

هو دليل لإجراء عمليات التدقيق وهو مخصص للمدققين الداخليين والخارجيين الذين يقومون بتقييم ISMSوفقًا لـ.ISO / IEC 27001

ISO/IEC 27007:2020أمن المعلومات والأمن السيبراني وحماية الخصوصية - إرشادات لتدقيق أنظمة إدارة أمن المعلومات

يعتمد الدليل بشكل كبير على دليل أنظمة إدارة التدقيق (ISO 19011) ويوفر إرشادات إضافية لنظام إدارة أمن المعلومات .(ISMS) .

الفصل الثالث

٣-١ الاستنتاجات :-

١. أهمية أمن المعلومات:

- يعد أمن المعلومات ضرورة أساسية لجميع المؤسسات، حيث تتعرض المعلومات الحساسة لمخاطر متعددة مثل الاختراقات والهجمات السيبرانية.
- تعزز المواصفات القياسية مثل ISO 27001 من أمان المعلومات وتساعد المؤسسات على حماية بياناتها.

٢. توافق القوانين واللوائح:

- تساهم معايير ISO في تحقيق الامتثال للمتطلبات القانونية والتنظيمية، مما يقلل من المخاطر القانونية والمالية.
- تضمن المؤسسات التي تطبق هذه المعايير أن تكون استراتيجياتها الأمنية متوافقة مع القوانين المعمول بها في مجال أمن المعلومات.

٣. تحسين سمعة المؤسسة:

- الحصول على شهادة ISO 27001 يمكن أن يعزز من سمعة المؤسسة ويزيد من ثقة العملاء والمستثمرين، مما قد يؤدي إلى ميزة تنافسية في السوق.
- توفر هذه الشهادات دليلًا موثقًا على التزام المؤسسة بأفضل الممارسات في أمن المعلومات.

٤. التقليل من التكاليف:

- يمكن أن يؤدي الاستثمار في نظام إدارة أمن المعلومات إلى تقليل التكاليف المرتبطة بالحوادث الأمنية من خلال الوقاية والتحكم في المخاطر.

٣-٢ التوصيات :

١. تطوير ثقافة أمن المعلومات:

- ينبغي على المؤسسات تعزيز الوعي بأهمية أمن المعلومات بين الموظفين وتوفير التدريب المستمر لهم.
- خلق بيئة ثقافية تدعم ممارسات الأمان وتعزز الالتزام الفردي والجماعي.

٢. تنفيذ استراتيجيات تقييم المخاطر:

- يجب أن تكون هناك استراتيجيات دورية لتقييم المخاطر وتحديث الضوابط الأمنية وفقًا للتغيرات في البيئة الداخلية والخارجية.
- الاستجابة السريعة للمخاطر المحتملة وتحليل الحوادث الأمنية السابقة لتحسين الأنظمة.

٣. الاستثمار في التكنولوجيا:

- ينبغي على المؤسسات استثمار في التقنيات الحديثة لحماية البيانات، مثل التشفير وأنظمة الكشف عن التسلل.
- استخدام الحلول الأمنية المتقدمة مثل الذكاء الاصطناعي لتحليل الأنماط وتحسين أمان المعلومات.

٤. الالتزام بالمواصفات القياسية:

- يُوصى بتطبيق معايير ISO 27001 وغيرها من المعايير ذات الصلة بشكل كامل، مع وضع خطة واضحة لتحقيق الشهادة.
- مراجعة دورية لمدى التزام المؤسسة بهذه المعايير لضمان الاستمرارية في تحسين الأمان المعلوماتي.

٥. التعاون مع الشركاء:

- من الضروري أن تتعاون المؤسسات مع الشركاء والموردين لتبادل المعرفة والخبرات حول أفضل الممارسات في أمن المعلومات.
- إنشاء شراكات استراتيجية لتعزيز أمان المعلومات عبر سلسلة التوريد.

المصادر :

١. الأحمدي، ع .(2020) .*أسس أمن المعلومات وحمايتها* .القاهرة: دار الكتب العلمية. (ص ٩٠) .

٢. الأحمدي، ع .(2020) .*أسس أمن المعلومات وحمايتها* .القاهرة: دار الكتب العلمية. (ص ٩٠) .

٣. صالح، م .(2021) .*استراتيجيات الحماية من الهجمات الإلكترونية* .الرياض: مكتبة الشروق. (ص ١١٢) .

٤. صالح، م .(2021) .*استراتيجيات الحماية من الهجمات الإلكترونية* .الرياض: مكتبة الشروق. (ص ١١٢) .

٥. الصقري، ج .(2022) .*تقنيات الكشف والوقاية من التسلل في الشبكات* .جدة: دار الفاروق. (ص ٦٨) .

٦. الصقري، ج .(2022) .*تقنيات الكشف والوقاية من التسلل في الشبكات* .جدة: دار الفاروق. (ص ٦٨) .

٧. العمري، م .(2019) .*تكنولوجيا المعلومات وأمنها* .الرياض: دار الكتاب الجامعي. (ص ٧٨) .

٨. العمري، م .(2019) .*تكنولوجيا المعلومات وأمنها* .الرياض: دار الكتاب الجامعي. (ص ٧٨) .

٩. القحطاني، ع .(2021) .*أمن المعلومات: المفاهيم والتطبيقات* .الرياض: دار الزهراء. (ص ٤٨) .

١٠. ISO 27001 متطلبات أنظمة إدارة أمن المعلومات، ISO/IEC 27001:2013 ، صفحة ٤- ١٣ .

11."Information Security Management Principles," by Andy P. McHugh et al., 2013, page 1.

12."ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements" [ISO.org, page 1].

13."ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements" [ISO.org, page 1].

14.Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley,p 109.

15.Calder , Alan & Watkins , Steve (2008). IT Governance a Manager’s Guide to Data Security and ISO27001/ISO 27002 (4th ed.). USA, Philadelphia : Replika Press,Pvt Ltd, p11.

16.ISO/IEC 27002:2022.

17.ISO/IEC 27002:2022.- Stallings, W. (2019). *Network Security: Principles and Practice*. Pearson. (p. 45).

18.Laudon, K. C., & Laudon, J. P. (2016). *Management Information Systems: Managing the Digital Firm*. Pearson, p15.

19. Parker, D. (1998). *Fighting Computer Crime: A New Framework for Protecting Information*. Wiley,p 44.

20. Parker, D. (2002). *Information Security: Principles and Practice*. Wiley,p27 .

21. Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton & Company , p 15 .

22. Stair, R., & Reynolds, G. (2017). *Principles of Information Systems*. Cengage Learning, p12.

23. Stallings, W. (2019). *Network Security: Principles and Practice*. Pearson. (p. 45).

24. Tipton, Harold F. & Krause, Micki (2006) Information Security Management Handbook (5th ed.) , United States of America : Taylor & Francis Group ،p7.